FAX COVER SHEET

From: Shakeel Mustafa
24831 Hendon Street
Laguna Hills, CA 92653
Tel: 949-457-1243

Subject:-

A List of New/Amended/Cancelled Claims

REF: Application/Control Number: 09/848,670

Attention: Ms. Courtney D. Fields

(Primary Patent Examiner)
Art Unit 2137
Fax # 1-703-872-9306
US Patent Office

Number of Pages 27 including this cover page

Date: April 3, 2005

A List of

New/Amended/Cancelled Claims

As Entered for the Application/Control Number 09/848,670

Section A:

The List of Claims as Filed With the Original Patent Application

Section B:

The Proposed List of New/Amended/Cancelled Claims

Section A:

The List of Claims as Filed With the Original Patent Application

1. A method for operating a digital information processing system that encrypts information from a plurality of remote processors to a host processor or vice versa the method comprising processor executed steps of: at the host and the remote processors before the start of encryption procedure: means for assigning and mutually agreeing upon, a pre-determined number of bits that are located at pre-determined and specific positions, called Group and Function Bits, within a seed binary bit segment consisting of any length; means for defining a plurality of function pool containing any type of mathematical or logical functions of any complexity; means for establishing a unique relationship between the functions defined in the first pool with the functions defined in the second pool sequentially identical at both the host and the remote processors; means for defining a number `N` which indicates the total number of rounds used for encryption/decryption process. at the remote processor: (a) means for generating and sending a seed arbitrary binary bit segment consisted of any length to the host processor; (b) means for processing the seed arbitrary binary bit segment at the remote processor; (c) means for producing a numeric number value based on the bit values of the Group and Function Bits as defined in the said arbitrary binary bit segment; (d) means for selecting a single or plurality of mathematical or logical functions from the first pool based upon the numeric number value of step (b); (e) means for identifying the corresponding single or plurality of mathematical or logical functions from the second pool; (g) means for encrypting the digital information segment through operating single or plurality of mathematical or logical functions selected from the second function pool as described in step d; (f) means for encrypting the arbitrary binary bit segment through operating single or plurality of mathematical or logical functions selected from the first pool as described in step c; (h) means for replacing the seed arbitrary binary bit segment with the encrypted arbitrary binary bit segment and using it as a new seed arbitrary binary bit segment; and (i) means for repeating the steps (b) to (h) `N` times and then transmitting the resulting encrypted digital information segment to the said host.

2. The method and system according to claim 1 wherein the said method comprising processor executed steps of: at the host processor: (a) means for receiving and identifying the seed arbitrary binary bit segment from the said remote processor; (b) means for processing the seed arbitrary binary bit segment; (c) means for producing a numeric number value based on the bit values of the Group and Function Bits as defined in the said arbitrary binary bit segment; (d) means for selecting a single or plurality of mathematical or logical functions from the first pool based upon the numeric number value of step (c); (e) means for identifying the corresponding single or plurality of mathematical or logical functions from the second pool; (f) means for identifying the corresponding inverse function for each of the mathematical or logical functions as recognized in step (e) and tabulating the identified inverse mathematical or logical functions entries; (g) means for encrypting the arbitrary binary bit segment through operating single or plurality of mathematical or logical functions selected from the first pool as described in step d; (h) means for replacing the seed arbitrary binary bit segment

with the encrypted arbitrary binary bit segment and using it as a new seed arbitrary binary bit segment; and (i) means for repeating the steps (b) to (h) `N` times and appending the inverse function entries resulting from each round into a tabular form.

3. The method and system according to claim 1 wherein the said method for operating a digital information processing system that decrypts information from a plurality of remote processors to a host processor or vice versa, the method comprising processor executed steps of: at the host processor: (a) means for receiving the encrypted digital information segment from the said remote processor; (b) means for decrypting the digital information segment with the last inverse mathematical function entry as found in the table built in step (i) of claim 2; (c) means for repeating the above step (b) until all the inverse mathematical or logical functions are exhausted as found in the built in table containing the inverse function entries.

4. The method and system according to claim 1 wherein the arbitrary binary bit segment can be a random number consisted of any arbitrary length.

5. The method and system according to claim 1 further comprising; means for encrypting a seed binary bit segment through operating mathematical or logical functions which can result in a large bit size number; and means for truncating the resulting large bit size number and reducing it to a pre-negotiated size mutually agreed between the said host and the remote.

6. The method and system according to claim 1 further comprising; means for re-using the encrypted seed binary bit segment resulting from the previous encrypted round as a new seed binary bit segment for the next encryption rounds; and means for encrypting the next digital information segments based on the information contained in the new seed binary bit segment.

7. The method and system according to claim 1 wherein the Group or Function Bits can mutually share the same single or plurality of bits located at pre-determined bit positions within a seed binary bit segment of any length.

8. The method and system according to claim 1 wherein any change in the Group or the Function Bits within a seed binary bit segment of any length leads to the selection of same or different set of mathematical or logical functions belonging to the first and second function pools.

9. The method and system according to claim 3 wherein the decryption procedure at the host processor comprises the steps of: means for identifying the exact same Group or Function Bits as identified by the remote processor through the use of seed arbitrary binary bit segment; means for identifying the exact same mathematical or logical functions from the first and the second function pools as identified by the remote processor; and means for identifying single or plurality of inverse mathematical or logical functions corresponding to each of the identified function from the second pool to be utilized for decryption procedure.

10. The method and system according to claim 1 wherein the Group and the Function Bits located within a seed binary bit segment of any length can be uniquely assigned and mutually recognized through the use of any mathematical or logical functions of any complexity.

11. The method and system according to claim 7 further comprising: means for reassigning and modifying the total number of Group and Function Bits within a seed binary bit segment in relation to the length range of the seed binary bit segment; and means for selecting and using the same or a different set of mathematical or logical functions based upon the length range of a seed binary bit segment.

12. The method and system according to claim 1 wherein the transmitted encrypted digital information may consist of different number of bits than the original digital information segment.

13. The method and system according to claim 12 wherein the transmitted encrypted digital information segment further comprising: means for containing a padding header followed by variable number of padding bit fields; and means for making the total encrypted digital information segment bits exactly divisible by a specific number.

14. The method and system according to claim 1 wherein the remote and host processors mutually adopt and agree upon the use of a set of protocols and instructions to exchange configuration parameters and system information comprising: means for reserving a specific bit at a pre-determined position in an information field such that the said bit value determines if the said information field is extended or span to include another known number of bits in the said field definition; means for exchanging and modifying the total number of Group and Function Bits and their corresponding bit positions assigned within a seed binary bit segment consisting of any arbitrary length; means for exchanging and modifying the unique association between Group or Function Bits numeric values and the corresponding mathematical or logical function; means for exchanging a seed binary bit segment or a random number consisting of any arbitrary length through the use of an instruction format being processed as a part of system information; and means for using or designing any type of protocols or instructions formats to exchange any type of system or configuration information.

15. The method and system according to claim 14 wherein the remote exchanges the system or configuration information with the host processor or vice versa comprising; means for receiving a public key from the host processor; means for encrypting any type of system or configuration information through using the public key of the host processor; means for transmitting the encrypted information to the host processor; and means for decrypting the said received information at the host through using the host's private key.

16. The method and system according to claim 13 wherein the mutually adopted and agreed upon set of protocols uses a reserved single bit field appended at a pre-determined

position known both to a host and a remote comprising, means for assigning the first outcome of the said bit value to indicate user's information, and means for assigning the second outcome of the said bit value to indicate system information.

17. The method and system according to claim 1 wherein the remote and host processors mutually agree on a procedure to verify the accuracy of encryption and decryption procedures, comprising: means for calculating and appending a unique digital signature field reflecting the information contents of a digital information segment before the start of the encryption procedure at the remote processor; means for calculating and verifying the same unique digital signature after decrypting the received digital information segment at the host processor; and means for initializing different set of procedures if the verification process fails.

18. A method and system according to claim 1 wherein the remote and host processors mutually agree on a procedure to verify that the encrypted digital information is being delivered to an authenticated processor and the encryption/decryption procedures are working properly, comprising: means for calculating and retaining a unique digital signature reflecting the information contents of a digital information segment before the start of the encryption procedure at the remote processor; means for calculating the same unique digital signature after decrypting the received digital information segment at the host processor; and means for encrypting and transmitting the said digital signature back to the originating remote processor; means for comparing and verifying the received digital signature with the retained digital signature at the remote processor; and means for initializing different set of procedures if the said verification process fails.

19. The method and system according to claim 1 wherein the type of digital information segment contains password information further comprising: means for using any information contained within a random number to identify and determine specific bit locations in an arbitrary binary bit segment; and means for mapping single or plurality of bits belonging to the password information segment into the said specific bit locations of the arbitrary binary bit segment.

20. The method and system according to claim 1 wherein the type of digital information segment contains authentication information further comprising: means for using any information contained within a password information segment to determine and identify specific bit locations in an arbitrary binary bit segment; and means for mapping single or plurality of bits belonging to a random number segment into the said specific bit locations of the arbitrary binary bit segment.

21. A method for operating a digital information processing system that encrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of: at the transmitting device: means for generating a seed random number consisting of any arbitrary length and transmitting the said random number to the receiving device; means for using the information contained in the random number to identify single or plurality of unique mathematical or logical functions identical at the both transmitting and the receiving devices; means for

encrypting any type of digital information consisted of any arbitrary length segment through operating the mathematical or logical functions; means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round; means for identifying the number of encryption rounds, N, through the use of any information means mutually agreed between the transmitting and the receiving devices; and means for repeating the encryption process on the said digital information segment and the said random number for N number of rounds.

22. A method for operating a digital information processing system that decrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of: at the receiving device: means for receiving and identifying the seed random number of an arbitrary length from the transmitting device; means for identifying the number of encryption rounds, N, through any means mutually agreed between the transmitting and the receiving devices; means for using the information contained within the specific bits of the seed random number to identify a single or plurality of unique mathematical or logical functions; means for identifying single or plurality of inverse functions corresponding to each of the identified mathematical or logical functions; means for decrypting the received digital information segment through operating single or plurality of inverse functions; means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round; and means for repeating the decryption process on the received digital information segment for N number of rounds to remove any effects of encryption on the said digital information segment.

Section B:

Amended/New Proposed Claims

(Original): Claim number 1 as filed with the application

~~1. A method for operating a digital information processing system that encrypts information from a plurality of remote processors to a host processor or vice versa the method comprising processor executed steps of: at the host and the remote processors before the start of encryption procedure: means for assigning and mutually agreeing upon, a pre-determined number of bits that are located at pre-determined and specific positions, called Group and Function Bits, within a seed binary bit segment consisting of any length; means for defining a plurality of function pool containing any type of mathematical or logical functions of any complexity; means for establishing a unique relationship between the functions defined in the first pool with the functions defined in the second pool sequentially identical at both the host and the remote processors; means for defining a number `N` which indicates the total number of rounds used for encryption/decryption~~

~~process. at the remote processor: (a) means for generating and sending a seed arbitrary binary bit segment consisted of any length to the host processor; (b) means for processing the seed arbitrary binary bit segment at the remote processor; (c) means for producing a numeric number value based on the bit values of the Group and Function Bits as defined in the said arbitrary binary bit segment; (d) means for selecting a single or plurality of mathematical or logical functions from the first pool based upon the numeric number value of step (b); (e) means for identifying the corresponding single or plurality of mathematical or logical functions from the second pool; (g) means for encrypting the digital information segment through operating single or plurality of mathematical or logical functions selected from the second function pool as described in step d; (f) means for encrypting the arbitrary binary bit segment through operating single or plurality of mathematical or logical functions selected from the first pool as described in step e; (h) means for replacing the seed arbitrary binary bit segment with the encrypted arbitrary binary bit segment and using it as a new seed arbitrary binary bit segment; and (i) means for repeating the steps (b) to (h) 'N' times and then transmitting the resulting encrypted digital information segment to the said host.~~

(Currently amended): Claim number 1 once amended and broken down into four claims as listed under claim numbers 1, 2, 3 and 4:

1. A method for encrypting and/or decrypting data segments from a plurality of remote processors to a host processor or vice versa. The method comprising the steps of:

at the host and the remote processors,

(a) mutually agreeing upon the locations of a pre-determined number of bits located within a random number of an arbitrary length through a set of pre-negotiated rules;

whereas, the said random number constituting in a binary format segment;

whereas, an arbitrary length of random number means the size of the random number that can be processed by the system resources utilized in the participating remote and host processor

(b) defining at least two pools containing mathematical or logical functions of arbitrary complexity; wherein:

(i) the first pool containing said functions that operate on random numbers;

(ii) the second pool containing said functions that operate on data segments that need to be encrypted; further

(iii) the second pool containing inverse functions such that every function defined in the second pool has an inverse function contained in it ;

(iv) the inverse functions for each of the functions contained in the second pool to be used in decrypting the data segments;

whereas, mathematical or logical functions of arbitrary complexity mean the functions that can be processed by the system resources utilized in the participating remote and host processor

(c) mutually agreeing upon the order of the functions defined in the first pool;

(d) mutually agreeing upon the order of the functions defined in the second pool;

(e) mutually agreeing upon establishing a unique relation between the functions defined in the first pool with the functions defined in the second pool;

for encrypting a data segment at the remote processor;

(f) generating a random number in a binary format with the segment length containing at least one bit location mutually agreed upon between remote and host in accordance with step (a);

(g) identifying the specific locations of bits in the random number as mutually agreed upon between the said host and remote processors as indicated in step (a);

(h) calculating the numeric values of the bits at the said specific locations;

(i) based on the result, identifying the functions from the first pool and the second pool;

(j) executing the functions as identified in the first pool to perform a round of encryption on the said random number;

(k) executing the functions as identified in the second pool to perform a round of encryption on the said data segment;

(l) replacing the encrypted random number as resulted in step (j) to be used in place of step (a)

(m) determining a number, N_T, that determines the total number of rounds of encryption from the information embedded in the said random number or in the encrypted versions of the random number;

(n) re-executing the procedure as described in steps (g) to (l) for N_T rounds of encryption;

(o) transmitting the said encrypted segment to the host processor;

at the host processor,

(p) receiving the said encrypted data segment from the remote processor;

(q) receiving thc random number as generated by the remote processor in step (f);

(r) identifying the specific bits' locations found within the said random number through the rules as mutually agreed upon in step (a);

(s) calculating the numeric values of the bits as found in the said specific locations;

(t) based on the result of step (s), identifying the functions set from the first pool;

(u) based on the result of step (s), identifying the inverse functions set from the second pool;

(v) executing the functions set as identified in the first pool to perform a first round of encryption on the said random number;

(w) executing the identified inverse functions set as identified in step (u) to perform a round of decryption on the said data segment;

(x) replacing the encrypted random number as resulted in step (v) in place of the random number as used in step (q);

(y) determining a number, N_T, that determines the total number of rounds of decryption from the information embedded in the said random number or in the encrypted versions of the random number;

(z) re-executing the procedure as described in steps (q) to (x) for N_T rounds of decryption; and

(aa) producing the decrypted data segment exactly to be the same as the original data segment before encryption.

(Currently amended): Claim number 2 filed as a part of the original claim number 1:

2. The method according to claim 1; further comprising;

between the host and the remote processors,

(a) identifying the length of the seed random number consisting of a binary segment;

(b) based on the length, mutually agreeing in advance through a set of rules on single or plurality of bits' locations found within the binary segment length of the said random number and calling them as Group Bits;

(c) calculating the numeric value of the Group Bits to further identify the unique locations of another bit set found within the binary segment length of the said random number and calling them as Function Bits;

(d) if the length of the random or encrypted random number changes, then optionally changing the locations of the bits constituting Group and Function Bits;

(e) with the rounds of encryption performed on the random number, optionally changing the locations of the bits constituting Group and Function Bits;

(f) with the rounds of encryption performed on the random number optionally changing the sequential order in which the functions defined in the first pool are organized; and

(g) with the rounds of encryption performed on the random number optionally changing the sequential order in which the functions defined in the second pool are organized.

(Currently amended): Claim number 3 filed as a part of the original claim number 1

3. The method according to claim 1; further comprising;

(a) defining an arbitrary range of mathematical or logical functions of arbitrary complexity in at least two pools, comprising;

in the first pool,

(b) populating the types of mathematical or logical functions of arbitrary complexity to be operated on random numbers in such a manner that enhance randomness characteristics of the random numbers;

(c) the types of functions selected in step (b), there may not necessarily exist inverse functions of the said functions chosen in the first pool;

in the second pool,

(d) populating the types of mathematical or logical functions of arbitrary complexity to be operated on data segments in such a manner that enhance randomness characteristics of the data segments; and

(e) the functions as selected in step (d), there must exist an inverse function for every function chosen in the said pool.

(Currently amended): Claim number 4 filed as a part of the original claim number 1:

4. The method according to claim 1, wherein the random number shared together by a host and a remote processor can consist of a known password.

(Original): Claim number 2 as filed with the application is hereby cancelled

~~2. The method and system according to claim 1 wherein the said method comprising processor executed steps of: at the host processor: (a) means for receiving and identifying the seed arbitrary binary bit segment from the said remote processor; (b) means for processing the seed arbitrary binary bit segment; (c) means for producing a numeric number value based on the bit values of the Group and Function Bits as defined in the said arbitrary binary bit segment; (d) means for selecting a single or plurality of mathematical or logical functions from the first pool based upon the numeric number value of step (c); (e) means for identifying the corresponding single or plurality of mathematical or logical functions from the second pool; (f) means for identifying the corresponding inverse function for each of the mathematical or logical functions as recognized in step (e) and tabulating the identified inverse mathematical or logical functions entries; (g) means for encrypting the arbitrary binary bit segment through operating single or plurality of mathematical or logical functions selected from the first pool as described in step d; (h) means for replacing the seed arbitrary binary bit segment with the encrypted arbitrary binary bit segment and using it as a new seed arbitrary binary bit segment; and (i) means for repeating the steps (b) to (h) `N` times and appending the inverse function entries resulting from each round into a tabular form.~~

(Original): Claim number 3 as filed with the application:

3. ~~The method and system according to claim 1 wherein the said method for operating a digital information processing system that decrypts information from a plurality of remote processors to a host processor or vice versa, the method comprising processor executed steps of: at the host processor: (a) means for receiving the encrypted digital information segment from the said remote processor; (b) means for decrypting the digital information segment with the last inverse mathematical function entry as found in the table built in step (i) of claim 2; (c) means for repeating the above step (b) until all the inverse mathematical or logical functions are exhausted as found in the built in table containing the inverse function entries.~~

(Currently amended): Claim number 3 once amended and broken into two claims listed under Claim No. 5 and Claim No. 6 as follows:

5. The method for encrypting data segments according to claim 1, wherein the said method builds up an encrypting table in advance containing a sequence of functions

to be used for encrypting data segments from a plurality of remote processors to the host processor or vice versa, the method comprising the steps of:

at the remote processor,

(a) generating a random number with the length containing the locations of Group and Function Bits;

(b) identifying the locations of the Group and Function Bits in the random number as found in the said specific locations within the random number;

(c) calculating the numeric value of the Group and Function Bits;

(d) based on the results of step (c), uniquely identifying a function from the first pool

(e) encrypting the random number through executing the function from the first pool as identified in step (d);

(f) calculating the numeric value of the Group and Function Bits;

(g) based on the results of step (f), uniquely identifying a function from the second pool;

(h) populating an encryption table by entering the function as identified in step (g) as the ith function entry into the said table;

(i) replacing the encrypted random number as resulted in step (e) to be used in place of step (a)

(j) determining a number, N_T, that determines the number of entries to be populated in the encryption table with the ith entry varying from 1 to N_T in the said table;

(k) re-executing the procedure as described in steps (a) to (i) for N_T of rounds to build the encryption table;

(l) identifying a data segment to be encrypted;

(m) encrypting the said data segment with the function entries as identified in the encryption table with the ith entry being as 1 to N_T of the said table; and

(n) producing an encrypted data segment.

6. A method for decrypting data segments according to claim 1, wherein the said method builds up a decryption table in advance containing a sequence of functions to be used for decrypting data segments from a plurality of remote processors to the host processor or vice versa, the method comprising the steps of:

at the host processor,

(a) receiving the random number as generated by the remote processor in step(a);

(b) identifying the locations of the Group and Function Bits in the random number as found in the said specific locations within the random number;

(c) calculating the numeric value of the Group and Function Bits;

(d) based on the results of step (c), uniquely identifying a function from the first pool

(e) encrypting the random number through executing the function from the first pool as identified in step (d);

(f) calculating the numeric value of the Group and Function Bits;

(g) based on the results of step (f), uniquely identifying a function from the second pool;

(h) based on the results of step (g), identifying the corresponding inverse function from the second pool;

(i) populating a decryption table by entering the inverse function as identified in step (h) as the ith function entry into the said table;

(j) replacing the encrypted random number as resulted in step (e) to be used in place of step (a);

(k) determining a number, N_T, that determines the number of entries to be populated in the decryption table with the ith entry varying from 1 to N_T in the said table;

(l) re-executing the procedure as described in steps (a) to (j) for N_T of rounds to build the decryption table;

(m) receiving the encrypted data segment from the remote processor;

(n) executing the function entries from ith entry being as N_T to 1 of the decryption table as built up in the step (l); and

(o) producing the decrypted data segment exactly to be the same as the original data segment before encryption.

(Original): Claim number 4 as filed with the application

4. ~~The method and system according to claim 1 wherein the arbitrary binary bit segment can be a random number consisted of any arbitrary length.~~

(Currently amended): Claim number 4 once amended as follows:

7. The method according to claim 1, wherein a random number can consist of an arbitrary binary bit segment of arbitrary length containing at least one Group and Function Bits.

(Original): Claim number 5 as filed with the application:

5. ~~The method and system according to claim 1 further comprising; means for encrypting a seed binary bit segment through operating mathematical or logical functions which can result in a large bit size number; and means for truncating the resulting large bit size number and reducing it to a pre-negotiated size mutually agreed between the said host and the remote~~.

(Currently amended): Claim number 5 once amended as follows:

8. The method according to claim 1; wherein encrypting a random number through operating mathematical or logical functions of the first pool further comprising;

(a) continuously monitoring the length of the random number as it is operated through a sequence of mathematical or logical functions contained in the first pool;

(b) if the length of the operated random number goes beyond a defined threshold, then truncating the length of the said random number to be contained within a pre-negotiated size mutually agreed upon between the said host and the remote processors.

(Original): Claim number 6 as filed with the application:

6. ~~The method and system according to claim 1 further comprising; means for re-using the encrypted seed binary bit segment resulting from the previous encrypted round as a new seed binary bit segment for the next encryption rounds; and means for encrypting the next digital information segments based on the information contained in the new seed binary bit segment~~.

(Currently amended): Claim number 6 once amended as follows:

9. The method according to claim 1; wherein a random number can be re-used for further encryption rounds comprising the steps of:

(a) re-using the encrypted random number resulting from the previous encrypted round and declaring it as a new seed random number;

(b) identifying Group and Function Bits from the said new random number; and

(c) based on the result of step (b), identifying the corresponding functions in the first and second pool;

(Original): Claim number 7 as filed with the application:

7. ~~The method and system according to claim 1 wherein the Group or Function Bits can mutually share the same single or plurality of bits located at pre-determined bit positions within a seed binary bit segment of any length~~.

(Currently amended): Claim number 7 once amended as follows:

10. The method according to claim 2; wherein the Group or Function Bits can mutually share the same single or plurality of bits located at pre-determined bit positions within a random number of an arbitrary length.

(Original): Claim number 8 as filed with the application:

8. ~~The method and system according to claim 1 wherein any change in the Group or the Function Bits within a seed binary bit segment of any length leads to the selection of same or different set of mathematical or logical functions belonging to the first and second function pools~~.

(Currently amended): Claim number 8 once amended as follows:

11. The method according to claim 2, wherein any change in the numeric values of Group or the Function Bits within a random number of arbitrary length leads to the selection of the same or different set of mathematical or logical functions belonging to the first and second function pools.

(Original): Claim number 9 as filed with the application is hereby cancelled

9. ~~The method and system according to claim 3 wherein the decryption procedure at the host processor comprises the steps of: means for identifying the exact same Group or Function Bits as identified by the remote processor through the use of seed arbitrary binary bit segment; means for identifying the exact same mathematical or logical functions from the first and the second function pools as identified by the remote processor; and means for identifying single or plurality of inverse mathematical or logical functions corresponding to each of the identified function from the second pool to be utilized for decryption procedure~~.

(Original): Claim number 10 as filed with the application:

10. ~~The method and system according to claim 1 wherein the Group and the Function Bits located within a seed binary bit segment of any length can be uniquely~~

~~assigned and mutually recognized through the use of any mathematical or logical functions of any complexity~~.

(Currently amended): Claim number 10 once amended as follows:

12. The method according to claim 2, wherein the exact locations of the Group and the Function Bits located within a seed or encrypted random number of arbitrary length can be uniquely assigned and mutually recognized between host and remote processors.

(Original): Claim number 11 as filed with the application:

11. ~~The method and system according to claim 7 further comprising: means for reassigning and modifying the total number of Group and Function Bits within a seed binary bit segment in relation to the length range of the seed binary bit segment; and means for selecting and using the same or a different set of mathematical or logical functions based upon the length range of a seed binary bit segment~~.

(Currently amended): Claim number 11 once amended as follows:

13. The method according to claim 2 further comprising:

(a) optionally re-assigning the locations of the Group and/or Function Bits in a mutually agreed manner between a participating host and remote processors as the length of the seed random number or the length of the encrypted random number changes;

(b) modifying the total number of Group and/or Function Bits in a mutually agreed manner within a seed or encrypted random number as the length of the seed random number or the length of the encrypted random number changes;

(c) based upon the results of step (a) and/or (b), selecting the same or different set of mathematical or logical functions from the first and/or the second pools.

(Original): Claim number 12 as filed with the application:

12. ~~The method and system according to claim 1 wherein the transmitted encrypted digital information may consist of different number of bits than the original digital information segment~~.

(Currently amended): Claim number 12 once amended as follows:

14. The method according to claim 1, wherein an encrypted data segment may consist of the same or different binary length containing more bits or less bits than the original un-encrypted version of the said data segment.

(b) exchanging and modifying the unique association between the Group and/or Function Bits numeric values and the corresponding mathematical or logical functions within the first and/or second pools;

(c) exchanging a seed binary bit segment or a random number consisting of an arbitrary length through the use of an instruction format being processed as a part of system information; and

(d) using or designing an arbitrary set of protocols or instruction formats to exchange system or configuration information.

(Original): Claim number 15 as filed with the application is hereby cancelled

15. ~~The method and system according to claim 14 wherein the remote exchanges the system or configuration information with the host processor or vice versa comprising; means for receiving a public key from the host processor; means for encrypting any type of system or configuration information through using the public key of the host processor; means for transmitting the encrypted information to the host processor; and means for decrypting the said received information at the host through using the host's private key~~.

(Original): Claim number 16 as filed with the application:

16. ~~The method and system according to claim 13 wherein the mutually adopted and agreed upon set of protocols uses a reserved single bit field appended at a pre-determined position known both to a host and a remote comprising, means for assigning the first outcome of the said bit value to indicate user's information, and means for assigning the second outcome of the said bit value to indicate system information.~~

(Currently amended): Claim number 16 once amended as follows:

17. The method according to claim 13, wherein, a remote processor engaged with a host processor in an encryption/decryption session distinguishes between a system/configuration related information segment and the user's related data segment through a reserved and mutually agreed upon single bit field known both to the host and remote processors, comprising;

(a) assigning the said bit field value of '0' to indicate user's information; and

(b) assigning the said bit field value of '1' to indicate system information.

(Original): Claim number 17 as filed with the application:

(Original): Claim number 13 as filed with the application:

13. ~~The method and system according to claim 12 wherein the transmitted encrypted digital information segment further comprising: means for containing a padding header followed by variable number of padding bit fields; and means for making the total encrypted digital information segment bits exactly divisible by a specific number~~.

(Currently amended): Claim number 13 once amended as follows:

15. The method according to claim 14, wherein the transmitted encrypted data segment is further comprised of:

(a) containing a padding header followed by a variable number of padding bits field; and

(b) choosing the number of bits in the padding field in a manner which makes the total bits in the encrypted data segment exactly divisible by a specific bit number.

(Original): Claim number 14as filed with the application:

14 ~~The method and system according to claim 1 wherein the remote and host processors mutually adopt and agree upon the use of a set of protocols and instructions to exchange configuration parameters and system information comprising: means for reserving a specific bit at a pre-determined position in an information field such that the said bit value determines if the said information field is extended or span to include another known number of bits in the said field definition; means for exchanging and modifying the total number of Group and Function Bits and their corresponding bit positions assigned within a seed binary bit segment consisting of any arbitrary length; means for exchanging and modifying the unique association between Group or Function Bits numeric values and the corresponding mathematical or logical function; means for exchanging a seed binary bit segment or a random number consisting of any arbitrary length through the use of an instruction format being processed as a part of system information; and means for using or designing any type of protocols or instructions formats to exchange any type of system or configuration information.~~

(Currently amended): Claim number 14 once amended as follows:

16. The method according to claim 1, wherein a remote processor engaged with a host processor in an encryption/decryption session can mutually exchange configuration parameters and system information comprising:

(a) exchanging and modifying the information about the total number of Group and Function Bits and their corresponding bit locations assigned within a seed random;

~~17. The method and system according to claim 1 wherein the remote and host processors mutually agree on a procedure to verify the accuracy of encryption and decryption procedures, comprising: means for calculating and appending a unique digital signature field reflecting the information contents of a digital information segment before the start of the encryption procedure at the remote processor; means for calculating and verifying the same unique digital signature after decrypting the received digital information segment at the host processor; and means for initializing different set of procedures if the verification process fails~~

(Currently amended): Claim number 17 once amended as follows:

18. The method according to claim 1 wherein, a remote processor engaged with a host processor in an encryption/decryption session mutually agrees on a procedure to verify the accuracy of encryption and decryption procedures, comprising:

at the remote processor,

(a) calculating the unique digital signature field rcflecting the information contents of a data segment;

(b) appending the unique digital signature field with the data segment in a packet format;

(c) encrypting the packet with the disclosed encryption techniques;

(d) transmitting the encrypted to the host processor;

at the host processor,

(e) receiving the encrypted packet;

(f) decrypting the packet;

(g) calculating the digital signature of the data segment

(h) verifying the digital signature by comparing the calculated digital signature with the received digital signature; and

(g) initializing the corrective procedures if the verification fails.

(Original): Claim number 18 as filed with the application:

~~18. A method and system according to claim 1 wherein the remote and host processors mutually agree on a procedure to verify that the encrypted digital information is being delivered to an authenticated processor and the encryption/decryption procedures are working properly, comprising: means for calculating and retaining a~~

~~unique digital signature reflecting the information contents of a digital information segment before the start of the encryption procedure at the remote processor; means for calculating the same unique digital signature after decrypting the received digital information segment at the host processor; and means for encrypting and transmitting the said digital signature back to the originating remote processor; means for comparing and verifying the received digital signature with the retained digital signature at the remote processor; and means for initializing different set of procedures if the said verification process fails.~~

(Currently amended): Claim number 18 once amended as follows:

19. The method according to claim 1 wherein a remote processor engaged with a host processor in an encryption/decryption session mutually agrees on a procedure to verify the accuracy of encryption and decryption procedures, comprising:

at the remote processor,

(a) encrypting a data segment with the disclosed encryption techniques;

(b) transmitting the encrypted data segment to the host processor;

at the host processor,

(c) receiving the encrypted data segment;

(d) decrypting the said data segment;

(e) calculating the digital signature of the received data segment;

(f) encrypting the digital signature with the disclosed encryption techniques;

(g) transmitting the encrypted digital signature to the said remote processor;

at the said remote processor,

(h) receiving the encrypted digital signature packet;

(i) decrypting the digital signature packet;

(j) calculating the digital signature of the original transmitted data segment;

(k) verifying the digital signature by comparing the calculated digital signature with the received digital signature; and

(l) initializing the corrective procedures if the verification fails.

(Original): Claim number 19 as filed with the application:

~~19. The method and system according to claim 1 wherein the type of digital information segment contains password information further comprising: means for using any information contained within a random number to identify and determine specific bit locations in an arbitrary binary bit segment; and means for mapping single or plurality of bits belonging to the password information segment into the said specific bit locations of the arbitrary binary bit segment.~~

(Currently amended): Claim number 19 once amended as follows:

20. The method according to claim 1, wherein password information between at least one host and remote processors can be transmitted as a type of data segment, comprising the steps of;

(a) using the information contained within a random number to identify and determine specific bit locations in an arbitrary binary bit segment; and

(b) mapping single or plurality of bits belonging to the password information segment into the said specific bit locations of the arbitrary binary bit segment.

(Original): Claim number 20 as filed with the application is herby cancelled:

~~20. The method and system according to claim 1 wherein the type of digital information segment contains authentication information further comprising: means for using any information contained within a password information segment to determine and identify specific bit locations in an arbitrary binary bit segment; and means for mapping single or plurality of bits belonging to a random number segment into the said specific bit locations of the arbitrary binary bit segment.~~

(Original): Claim number 21 as filed with the application:

21. ~~A method for operating a digital information processing system that encrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of: at the transmitting device: means for generating a seed random number consisting of any arbitrary length and transmitting the said random number to the receiving device; means for using the information contained in the random number to identify single or plurality of unique mathematical or logical functions identical at the both transmitting and the receiving devices; means for encrypting any type of digital information consisted of any arbitrary length segment through operating the mathematical or logical functions; means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round; means for identifying the number of encryption rounds, N, through the use of any information means mutually agreed between the transmitting and the receiving devices; and means for repeating the encryption~~

~~process on the said digital information segment and the said random number for N number of rounds.~~

(Currently amended): Claim number 21 once amended as follows:

21 A method for encrypting/decrypting data segments from a plurality of transmitting devices to a receiving device or vice versa. The method comprising the steps of:

at the transmitting and receiving devices,

(a) defining a first set containing mathematical and/or logical functions;

(b) defining a second set containing the inverse functions of every function defined in the first set as indicated in step (a);

(c) agreeing upon a set of rules to identify a single or plurality of specific bits locations present within a random number;

(d) sharing a random number long enough to contain a single or plurality of specific bits locations as mutually agreed upon in step (c);

wherein, a random number constitutes a binary segment of arbitrary length

(e) agreeing upon the sequential order in which the functions defined in the first set are organized;

(f) establishing one-to-one mapping between the functions defined in the first set with their corresponding inverse functions defined in the second set

at the transmitting devices,

(g) using information embedded within the random number to identify a function in the first set to:

(h) encrypting the random number;

(i) encrypting the data segment;

(j) replacing the encrypted random number resulted in step (h) to be used in place of step (g)

(k) determining a number, N_T, that determines the encryption rounds on the said random number and the data segment;

(l) re-executing step (g) to step (j) for N_T number of rounds at the receiving devices,

(m) using the information embedded within the random number to identify a function in the first set to:

(n) encrypting the random number;

(o) identifying the inverse function from the second set that corresponds to the function used in the first set as identified in step (m);

(p) using the said inverse function from the second set to;

(q) decrypting the received data segment;

(r) replacing the encrypted random number resulted in step (n) to be used in place of step (m)

(s) determining a number, N_T, that determines the encryption rounds on the random number and the decryption rounds on the data segment;

(t) re-executing step (m) to step (r) for N_T number of rounds;

(u) producing the decrypted data segment exactly to be the same as the original data segment before encryption.

21 ~~A method for operating a digital information processing system that decrypts information from a plurality of transmitting devices to a receiving device or vice versa the method comprising processor executed steps of: at the receiving device: means for receiving and identifying the seed random number of an arbitrary length from the transmitting device; means for identifying the number of encryption rounds, N, through any means mutually agreed between the transmitting and the receiving devices; means for using the information contained within the specific bits of the seed random number to identify a single or plurality of unique mathematical or logical functions; means for identifying single or plurality of inverse functions corresponding to each of the identified mathematical or logical functions; means for decrypting the received digital information segment through operating single or plurality of inverse functions; means for encrypting the seed random number through operating the mathematical or logical functions and declaring the resulting number as the seed random number for the next round; and means for repeating the decryption process on the received digital information segment for N number of rounds to remove any effects of encryption on the said digital information segment.~~

(Currently amended): Claim number 21 once amended as follows:

22. A method for encrypting and/or decrypting data segments from a plurality of remote processors to a host processor or vice versa. The method comprising the steps of:

at the host and the remote processors,

(a) defining a first set containing mathematical and/or logical functions;

(b) defining a second set containing mathematical and/or logical functions and their corresponding inverse functions;

(c) sharing an identical password constituting a binary segment of arbitrary length;

(d) using the information embedded in the said password identifying a function contained in the first set;

(e) populating the first column of a table by entering the function as identified from the first set in step (d) as the ith function entry into the said table;

(f) encrypting the password with the function as identified in step (e);

(g) using the information embedded in the password to identify a function contained in the second set;

(h) populating the second column of the said table by entering the function identified from the second set in step (g) as the jth function entry into the said table;

(i) populating the third column of the said table by entering the inverse function of the function as identified from the second set in step (g) as the jth inverse function entry into the said table;

(j) replacing the encrypted password as resulted in step (f) to be used in place of step (c)

(k) determining a number, N_T, that determines the number of entries in the first, second and third columns of the said table;

(l) re-executing step (c) to step (j) for N_T number of rounds;

at the remote processor,

(m) determining a number, E_R, which determines the number of encryption rounds to be performed on a data segment such that $1 < E_R < N_T$;

(n) encrypting a data segment by using the functions as listed under the second column with the ith function entry being vary from 1 to E_R number of encryption rounds;

(o) transmitting the encrypted data segment produced by step (n) to the host processor;

at the host processor,

(p) receiving the said encrypted data segment resulting from step (o);

(q) determining a number, D_R, which determines the number of decryption rounds to be performed on the received encrypted data segment such that $D_R = E_R$, and

(r) decrypting the said data segment by using the inverse functions as listed under the third column with the jth function entry varying being vary from 1 to D_R number of decryption rounds;

(s) producing the decrypted data segment exactly to be the same as the original data segment before encryption.

(New): Claim number 23 being filed as new Claim with the application:

23. The method according to claim 22, wherein at least one host and remote processors can mutually authenticate through encrypting/decrypting random numbers, comprising the steps of:

at the remote processor,

(a) generating a random number, R_A;

(b) determining a sequence of functions to encrypt the random number R_A through the disclosed encryption techniques producing encrypted random number R_{AE};

(c) transmitting the encrypted random number R_{AE} to the host processor

at the host processor,

(d) receiving the encrypted random number R_{AE}

(e) decrypting the random number R_{AE} with a sequence of inverse functions through the disclosed decryption techniques producing R_A;

(f) determining a sequence of functions in the opposite order as to step (b) to encrypt the random number R_A to produce R_{EA};

(g) transmitting the encrypted random number R_{EA} to the remote processor

at the remote processor,

(h) receiving the encrypted random number R_{EA}

(i) determining a sequence of functions in the opposite order as to step (b) to encrypt the random number R_A to produce $R_{EA;}$

(j) if the result of step (h) and (i) matches, then authenticating the host processor